

Claims

What is claimed is:

1. A method for promoting compliance with data protection and privacy laws and regulations relating to the privacy rights of individuals that comprises:

5 informing an individual involved in potential disclosure of his/her personal data to an entity that the entity has certified its compliance with approved privacy and data security practices that conform to relevant data protection and privacy laws and regulations covering the use of personal data in at least the individual's or the entity's country of location;

10 obtaining the individual's consent to have the entity receive, or acknowledgment that the entity will receive, and use his/her personal data in accordance with a stated policy or with relevant data protection and privacy laws and regulations covering the use of personal data in at least the individual's or the entity's country of location;

15 transmitting to the entity data indicating that the individual has been informed of the entity's privacy practices and consented to the entity receiving, or acknowledged that the entity will be receiving, and using his/her personal data in accordance with its stated policy or with relevant data protection and privacy laws and regulations covering the use of personal data in at least the individual's or the entity's country of location;

receiving from the entity data comprising personal data collected by the entity from the individual;

20 storing said personal data received from the entity; and

periodically checking whether the entity has complied with the stated policy or with relevant data protection and privacy laws and regulations covering the use of personal data in at least the individual's or the entity's country of location.

25 2. A method according to claim 1 further comprising the step of informing the individual that the entity is covered by insurance or equivalent risk instrument to protect against risk of loss or harm caused to the individual arising from misuse or loss of the individual's personal data by the entity.

30 3. A method according to claim 1 wherein said data indicating that the

individual has consented to have the entity receive, or acknowledgment that the entity will receive, and use the individual's personal data comprises data uniquely identifying details relating to the individual's consent.

5 4. A method according to claim 3 wherein said data indicating that the individual has consented to have the entity receive, or acknowledgment that the entity will receive, and use the individual's personal data and uniquely identifying details relating to the individual's consent is compressed using a hash function.

10 5. A method according to claim 4 wherein said data received from the entity comprising personal data collected by the entity from the individual includes the data transmitted to the entity uniquely identifying details relating to the individual's consent.

15 6. A method according to claim 1 performed with a multiplicity of entities and individuals located in a single country.

20 7. A method according to claim 1 performed with a multiplicity of entities and individuals located in a multiplicity of countries.

25 8. A method according to claim 1 wherein the individual is informed in an official language of the individual's country of location.

30 9. A method according to claim 1 conducted as a multi-entity privacy policy certification program requiring member entities to certify compliance with approved privacy standards for the use of personal data of individuals and providing such entities with a policy notice to confirm their approval by, and membership in, the program.

 10. A method according to claim 9 wherein the approved standards meet the standards required by the United States, European Union, or other countries or regional organizations.

11. A method according to claim 9 further comprising the step of having audits or other assessments performed upon entities seeking or having membership in the privacy policy certification program to ensure that the entities' privacy practices satisfy the standards approved and required by the program.

5

12. A method according to claim 11 further comprising the step of having random inspections or audits performed upon member entities to verify compliance by the entities with their approved privacy practices.

10

13. A method according to claim 12 wherein, upon discovery of a violation of an entity's approved privacy practices, notice thereof and a request for correction are provided to the entity.

15

14. A method according to claim 13 wherein, upon failure by an entity to comply with a request for correction, the entity's policy notice is extinguished.

20

15. A method according to claim 14 wherein, upon any continued improper use of the policy notice by the entity, an enforcement action to terminate such use is initiated and notice thereof is provided to an appropriate regulatory authority.

25

16. A method according to claim 1 wherein the data received from the entity comprising the individual's stored personal data includes the time period of the individual's consent or acknowledgment, the length of time that the individual's personal data will be retained, and an option to extend or renew the individual's consent or acknowledgment, if desired, notice thereof being provided to the entity and the individual in advance of expiration of the consent.

30

17. A method according to claim 16 wherein the individual is provided with the option of having the individual's personal data deleted from the entity's data storage upon expiration of the agreement.

18. A method according to claim 2 wherein as prerequisites to membership in the privacy policy certification program, an entity is required to agree to (a) work with providers of insurance or equivalent risk instruments to resolve disputes with individuals, and (b) reimburse providers of insurance or equivalent risk instruments for claims paid to individuals
5 due to violations of the their privacy rights by the entity.

19. A method according to claim 1, wherein the steps of informing the individual, obtaining the individual's consent or acknowledgment, transmitting data to the entity, and receiving data from the entity are performed over a computer network.

20. A method according to claim 19 wherein the computer network is the Internet.

21. A system for promoting compliance with data protection and privacy laws and regulations relating to the privacy rights of individuals that comprises:

means for informing an individual involved in potential disclosure of his/her personal data to an entity that the entity has certified its compliance with approved privacy and data security practices that conform to relevant data protection and privacy laws and regulations covering the use of personal data in at least the individual's or the entity's country of
20 location;

means for obtaining the individual's consent to have the entity receive, or acknowledgment that the entity will receive, and use his/her personal data in accordance with a stated policy or with relevant data protection and privacy laws and regulations covering the
25 use of personal data in at least the individual's or the entity's country of location;

means for transmitting to the entity data indicating that the individual has been informed of the entity's privacy practices and consented to the entity receiving, or acknowledgment that the entity will be receiving, and using his/her personal data in
30 accordance with its stated policy or with relevant data protection and privacy laws and

regulations covering the use of personal data in at least the individual's or the entity's country of location;

5 means for receiving from the entity data comprising personal data collected by the entity from the individual;

means for storing said personal data received from the entity; and

10 means for periodically checking whether the entity has complied with the stated policy or with relevant data protection and privacy laws and regulations covering the use of personal data in at least the individual's or the entity's country of location.

22. A system according to claim 21 further comprising means for informing the individual that the entity is covered by insurance or equivalent risk instrument to protect
15 against risk of loss or harm caused to the individual arising from misuse or loss of the individual's personal data by the entity.

23. A system according to claim 21 wherein said data indicating that the individual has consented to have the entity receive, or acknowledgment that the entity will
20 receive, and use the individual's personal data comprises data uniquely identifying details relating to the individual's consent.

24. A system according to claim 23 wherein said data indicating that the individual has consented to have the entity receive, or acknowledgment that the entity will
25 receive, and use the individual's personal data and uniquely identifying details relating to the individual's consent is compressed using a hash function.

25. A system according to claim 24 wherein said data received from the entity comprising personal data collected by the entity from the individual includes the data
30 transmitted to the entity uniquely identifying details relating to the individual's consent.

26. A system according to claim 21 wherein the individual is informed in an official language of the individual's country of location.

27. A system according to claim 21 comprising means for conducting a multi-entity privacy policy certification program requiring member entities to certify compliance with approved privacy standards for the use of personal data of individuals and means for providing such entities with a policy notice to confirm their approval by, and membership in, the program.

28. A system according to claim 27 wherein the approved standards meet the standards required by the United States, European Union, or other countries or regional organizations.

29. A system according to claim 27 further comprising means for having audits or other assessments performed upon entities seeking or having membership in the privacy policy certification program to ensure that the entities' privacy practices satisfy the standards approved and required by the program.

30. A system according to claim 29 further comprising means for having random inspections or audits performed upon member entities to verify compliance by the entities with their approved privacy practices.

31. A system according to claim 30 further comprising means for providing notice to an entity of a violation of the entity's approved privacy practices upon discovery thereof and means for providing a request for correction to the entity.

32. A system according to claim 31 further comprising means for extinguishing an entity's policy notice upon failure by the entity to comply with a request for correction.

33. A system according to claim 32 further comprising means for, upon any continued improper use of a policy notice by an entity, providing to an appropriate regulatory

authority notice of such improper use, and initiating an enforcement action to terminate such use.

34. A system according to claim 21 wherein the data received from the entity comprising the individual's stored personal data includes the time period of the individual's consent or acknowledgment, the length of time that the individual's personal data will be retained, and an option to extend or renew the individual's consent or acknowledgment, if desired, notice thereof being provided to the entity and the individual in advance of expiration of the consent.

35. A system according to claim 34 further comprising means for providing the individual with the option of having the individual's personal data deleted from the entity's data storage upon expiration of the agreement.

36. A system according to claim 22 wherein as prerequisites to membership in the privacy policy certification program, an entity is required to agree to (a) work with providers of insurance or equivalent risk instruments to resolve disputes with individuals, and (b) reimburse providers of insurance or equivalent risk instruments for claims paid to individuals due to violations of the their privacy rights by the entity.

37. A system according to claim 21, wherein the means for informing the individual, obtaining the individual's consent or acknowledgment, transmitting data to the entity, and receiving data from the entity comprise a computer network.

38. A system according to claim 37 wherein the computer network is the Internet.